



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,213	02/05/2002	Siani Lynne Pearson	B-4488PCT 619500-7	8050

22879 7590 01/17/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

AVERY, JEREMIAH L

ART UNIT	PAPER NUMBER
----------	--------------

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	01/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/049,213
Filing Date: February 05, 2002
Appellant(s): PEARSON ET AL.

MAILED

JAN 17 2007

Technology Center 2100

Robert Popa Reg. No. 43,010
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/18/06 appealing from the Office action mailed 04/26/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The Examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The Appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the Examiner. The 35 U.S.C. 101 provisional double patenting rejection of claim 27.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,943,423	Muftic	8-1999
6,091,835	Smithies et al.	7-2000
5,870,723	Pare, Jr. et al.	2-1999

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-15, 18-22, 24, 26-44 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,943,423 to Muftic, hereinafter Muftic.

1. (Original) Regarding claims 1, 18 and 27, Muftic discloses a computer system adapted to restrict operations on data, comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data (column 3, lines 46-67, column 4, lines 1-10 and column 5, lines 23-54);

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

[Performing "cryptographic functions and transformations" assists in protecting the contents found in the trusted module ("smart token").]
an access profile specifying license permissions of users with respect to the data (column 5, lines 48-54);
wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present (column 5, lines 55-67 and column 6, lines 1-4, 19-31).

2. (Original) Regarding claims 2 and 28, Muftic discloses wherein the computer platform further comprises a platform trusted module and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication (Figure 1, column 3, lines 46-61, column 5, lines 30-47, column 7, lines 61-67 and column 8, lines 1-23).
3. (Original) Regarding claims 3, 29 and 42, Muftic discloses wherein some or all of the functionality of the secure operator is within the platform trusted module (column 3, lines 46-67 and column 4, lines 1-5).
4. (Original) Regarding claims 4 and 30, Muftic discloses wherein the access profile is within the computer platform (column 5, lines 30-47).
5. (Original) Regarding claims 5 and 31, Muftic discloses wherein some or all of the data is within the computer platform and the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries

out operations on the data (column 3, lines 58-67, column 4, lines 1-5 and column 6, lines 31-31).

6. (Original) Regarding claim 6, Muftic discloses wherein some or all of the data is within the portable trusted module or in a device containing the portable trusted module and the portable trusted module or the device containing the portable trusted module further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (column 6, lines 32-42, 47-49).

7. (Original) Regarding claims 7, 32 and 43, Muftic discloses wherein the data protector is within the relevant trusted module (column 3, lines 46-67, column 4, lines 1-5 and column 6, lines 31-31).

8. (Original) Regarding claims 8, 33 and 44, Muftic discloses wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the relevant trusted component (column 8, lines 61-67, column 9, lines 1-17, 40-57).

9. (Original) Regarding claims 9 and 34, Muftic discloses wherein the trusted platform is adapted at boot to check the integrity of operation protection code comprising the secure operator and, if present, the data protector (column 5, lines 55-67, column 6, lines 1-4 and column 9, lines 7-13).

10. (Original) Regarding claim 10, Muftic discloses wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication and wherein the computer platform is adapted to perform the integrity check by reading and hashing the

Art Unit: 2131

operation protection code to produce a first hash, reading and decrypting a stored signed version of a secure operation protection code hash using a public key certificate of a third party stored in the platform trusted module to produce a second hash, and comparing the first has and the second hash (Figure 1, column 3, lines 46-61, column 5, lines 30-67, column 6, lines 1-4, column 7, lines 61-67, column 8, lines 1-23, column 15, lines 66 and 67 and column 16, lines 1-15 and 35-46).

11. (Original) Regarding claim 11, Muftic discloses wherein the portable trusted module contains a user access license specifying access rights to the data associated with the removable trusted module, whereby unless prevented by the access profile, the secure operator is adapted to check the user access license to determine whether a requested operation is licensed for the user identity contained in the portable trusted module (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10, column 5, lines 48-67 and column 6, lines 1-4, 19-49).

12. (Original) Regarding claims 12 and 35, Muftic discloses wherein the computer platform comprises a secure communication path between the platform trusted module and the operating system of the computer platform (column 5, lines 30-47 and column 8, lines 12-22).

13. (Currently Amended) Regarding claims 13 and 36, Muftic discloses wherein the computer platform is adapted such that:

the operating system requests a policy check from the secure operator before acting upon the data, by sending the name of the target data plus the intended operation (column 9, lines 47-57 and column 10, lines 38-41);

the secure operator checks the restrictions associated with the target data in the access profile, to determine whether the data may be operated upon (column 5, lines 55-67 and column 6, lines 1-4, 19-31);

the secure operator checks the proposed usage with the restrictions, and replies to the operating system (column 5, lines 48-54).

14. (Currently Amended) Regarding claims 14 and 37, Muftic discloses wherein the computer platform further comprises a platform trusted module, wherein the platform trusted module and the portable trusted module are adapted for mutual authentication and wherein some or all of the functionality of the secure operator is within the platform trusted module (Figure 1, column 3, lines 46-67, column 4, lines 1-5, column 5, lines 30-47, column 7, lines 61-67 and column 8, lines 1-23);

wherein on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested (column 5, lines 48-67, column 6, lines 1-4, 21-31 and column 10, lines 5-20).

Art Unit: 2131

15. (Original) Regarding claim 15, Muftic discloses wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, and wherein the computer system further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (Figure 1, column 3, lines 46-67, column 4, lines 1-5 column 5, lines 30-47, column 6, lines 31-31, column 7, lines 61-67 and column 8, lines 1-23);

wherein the relevant trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result (Figure 22, column 5, lines 55-67, column 6, lines 1-4, 21-31 and column 16, lines 35-46).

16. (Original) Regarding claim 19, Muftic discloses wherein the operating system of the computer platform is adapted to request a policy check from the access controller before carrying out certain operations on the data, whereupon the access controller checks restrictions applying to the data to determine whether the data may be operated on, and replies to the operating system accordingly (column 5, lines 30-67 and column 6, lines 1-4 ad 21-31).

17. (Currently Amended) Regarding claim 20, Muftic teaches a method of restricting operations on data in a system comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data (column 3, lines 46-67, column 4, lines 1-10 and column 5, lines 23-54);

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

an access profile specifying license permissions of users with respect to the data (column 5, lines 48-54);

the method comprising a request for a policy check by the operating system of the computer platform to the secure operator before acting upon the data, by sending to the secure operator the name of the target data plus the intended operation (column 9, lines 47-57 and column 10, lines 38-41);

the secure operator checking the restrictions associated with the target data in the access profile to determine whether the data may be operated upon (column 5, lines 55-67 and column 6, lines 1-4, 19-31);

the secure operator checking the proposed usage with the restrictions, and replying to the operating system (column 5, lines 48-54).

Art Unit: 2131

18. (Original) Regarding claim 21, Muftic teaches wherein the computer platform further comprises a platform trusted module, and wherein some or all of the functionality of the secure operator is within the platform trusted module, and whereby on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator, whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested (column 3, lines 46-67, column 4, lines 1-5, column 5, lines 48-67, column 6, lines 1-4, 21-31 and column 10, lines 5-20).

19. (Original) Regarding claim 22, Muftic teaches wherein the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data, and wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result (Figure 22, column 3, lines 58-67, column 4, lines 1-5, column 5, lines 55-67, column 6, lines 1-4, 31-31 and column 16, lines 35-46).

20. (Original) Regarding claim 24, Muftic teaches wherein the computer platform comprises a secure communication path between the platform trusted component and the operating system, and whereby the request from the secure operator to the

Art Unit: 2131

operating system to use the data is provided on the secure communication path (column 5, lines 30-47 and column 8, lines 12-22, 32-34).

21. (Original) Regarding claim 26, Muftic teaches a method of installing data on to a computer platform for restricted use thereon, the computer platform comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data, a platform trusted module wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification, and a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (column 3, lines 38-67, column 4, lines 1-10, column 5, lines 23-54 and column 6, lines 32-49); the method comprising verification of the reliability of the data before installation of the data and an associated access profile, and loading of a digest of protected data and an associated access profile into the platform trusted module, whereby the digest is used by the data protector and/or secure operator before execution of the data (column 8, lines 61-67, column 9, lines 1-17, 40-57).

22. (Original) Regarding claim 38, Muftic discloses a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector

Art Unit: 2131

prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result (Figure 1, column 3, lines 46-61, column 5, lines 30-47, 55-67, column 6, lines 1-4, 31-31, column 7, lines 61-67, column 8, lines 1-23 and column 16, lines 35-46).

23. (Currently Amended) Regarding claim 39, Muftic discloses a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

the portable trusted module containing a user access license specifying access rights to data associated with the portable trusted module (column 5, lines 48-54).

24. (Original) Regarding claim 40, Muftic discloses a portable trusted module located within a smart card (column 2, lines 28-30, column 3, lines 26-28, 38-45 and column 4, lines 6-10).

25. (Original) Regarding claim 41, Muftic teaches a method of restricting operations on data in a system comprising:

a computer platform having an access controller specifying license permissions of users with respect to the data (column 5, lines 23-54, "set of privileges");

enabling use of the data (column 5, lines 48-54, "authorizing the activity");

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

the method comprising a request for a policy check by the operating system of the computer platform to the access controller before acting upon the data, by sending to the access controller the name of the target data plus the intended operation (column 9, lines 47-57 and column 10, lines 38-41);

the access controller checking the restrictions associated with the target data to determine whether the data may be operated upon (column 5, lines 55-67 and column 6, lines 1-4, 19-31);

replying to the operating system (column 5, lines 48-54, column 6, lines 25-31). [A response is given in the form of "authorizing" or denying access to the data.]

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2131

26. (Original) Claims 16 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic as applied to claims 2 and 21 above (respectively), and further in view of U.S. Patent No. 6,091,835 to Smithies et al., hereinafter Smithies.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

27. As per claims 16 and 25, Muftic discloses the invention substantially as claimed in claims 2 and 21, respectively, but fails to disclose wherein the platform trusted component is adapted to log requests to the operating system to perform particular operations on the data.

28. However, Smithies discloses wherein the platform trusted component is adapted to log requests to the operating system to perform particular operations on the data (column 11, lines 51-67, column 16, lines 39-60, column 19, lines 16-24, column 26, lines 37-42, column 27, 49-60, column 42, lines 53-67 and column 43, lines 1-11).

29. The motivation to do so would be to "confirm specifics such as that the affirming party is in fact the identified party" (Smithies - column 7, lines 23-25, column 8, lines 15-43, column 9, lines 64-67 and column 10, lines 1-13).

30. Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Smithies within the system of

Art Unit: 2131

Muftic to obtain the claimed invention because it would restrict access to the desired data, document, etc. to only those possessing authorized access credentials.

31. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic as applied to claim 6 above, and further in view of U.S. Patent No. 6,091,835 to Smithies et al., hereinafter Smithies.

32. As per claim 17, Muftic discloses the invention substantially as claimed in claim 6, but fails to disclose wherein the portable trusted component is adapted to log requests to the operating system to perform particular operations on the data.

33. However, Smithies discloses wherein the portable trusted component is adapted to log requests to the operating system to perform particular operations on the data (column 11, lines 51-67, column 16, lines 39-60, column 19, lines 16-24, column 26, lines 37-42, column 27, 49-60, column 42, lines 53-67 and column 43, lines 1-11).

34. The motivation to do so would be to "confirm specifics such as that the affirming party is in fact the identified party" (Smithies - column 7, lines 23-25, column 8, lines 15-43, column 9, lines 64-67 and column 10, lines 1-13).

35. Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Smithies within the system of Muftic to obtain the claimed invention because it would restrict access to the desired data, document, etc. to only those possessing authorized access credentials.

36. (Original) Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic as applied to claim 21 above, and further in view of U.S. Patent No. 5,870,723 to Pare et al., hereinafter Pare.

37. As per claim 23, Muftic discloses the invention substantially as claimed in claim 21, but fails to teach wherein before execution of the data, the data protector checks that there are not multiple copies of the data stored within the computer platform and prevents data execution if there are multiple copies.

38. However, Pare teaches wherein before execution of the data, the data protector checks that there are not multiple copies of the data stored within the computer platform and prevents data execution if there are multiple copies (column 13, lines 12-19, 26-49). Pare only allows one copy of data and other software to be stored, thus preventing multiple copies from existing.

39. The motivation to do so would be "that even successful capture and dissection of a given future key table does not reveal messages that were previously sent" (column 19, lines 43-57).

40. Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Pare within the system of Muftic to obtain the claimed invention because it would better resist attempts to obtain access to protected via a stolen access code, identifier, credential, etc.

(10) Response to Argument

Issue 1: With regards to the amendments to the drawings, the Examiner accepts said amendments, pending the submission of corrected drawing sheets.

Issue 2: Regarding the Appellant's assertion that Muftic fails to disclose "an access profiles specifying license permissions of users" or "an access controller for specifying license permissions of users", the Examiner respectfully disagrees and maintains that

such disclosure is found within Muftic. In column 5, lines 23-54, the “authorization credentials” correspond to the Appellant’s “access profile”. Credentials comprise basic identifying information about a user. A profile comprises information pertaining to a description of a user or group of users. Thus, the “credentials” disclosed by Muftic and the “profile” claimed by the Appellant are synonymous.

Pertaining to the “license permissions”, Muftic discloses “a method of authorizing an activity in a computing environment only to those persons authorized to engage in the activity” and further, “if an authorizing credential is found, authorizing the activity”. The act of authorizing said “activity in a computing environment” is akin to the functionality of identifying the specific usage rights that are granted to a particular user, which is a fundamental concept behind the utilization of “license permissions”.

With regards to the “portable trusted module”, the disclosure by Muftic of “smart tokens” that can be smart cards or PCMCIA cards; of which “one smart token is programmed to perform cryptographic functions and transformations based on at least one cryptographic algorithm” as found in the following sections of Muftic, (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49). The performance of cryptographic functions provide a secure environment for the data to reside. Furthermore, it is known in the art that a smart card is a portable, updatable card that can be used to store an assortment of data; thus the disclosed smart card constitutes the Appellant’s claimed “portable trusted module”.

Pertaining to claim 20, Appellant’s inquiry as to where does Muftic disclose “a set of credentials and identification means are stored and associated with each user”, the

Examiner asserts that no such limitation is found within the claim language of Appellant's claim 20.

Regarding claim 41, an access control methodology is found within the teachings of Muftic, in particular but not limited to column 5, lines 23-67, "A signature associated with access credentials used for user authorization is validated before access is granted", "a method of preventing use of software modified without authorization and unauthorized access to software without possession of a smart token" and column 6, lines 1-20, "distributing one user authorization credential with each authorized copy of the software; and preventing the possibility to activate the copy of the software without using a valid user authorization credential."

Issue 3: Regarding the 35 U.S.C. 103(a) rejection of claims 16, 17 and 25, the Examiner maintains that the combination of the teachings of Muftic and Smithies teaches the claimed invention. The motivation to do so would be to "confirm specifics such as that the affirming party is in fact the identified party" (Smithies - column 7, lines 23-25, column 8, lines 15-43, column 9, lines 64-67 and column 10, lines 1-13).

Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Smithies within the system of Muftic to obtain the claimed invention because it would restrict access to the desired data, document, etc. to only those possessing authorized access credentials.

Issue 4: Due to the Appellant's failure to address the 35 U.S.C. 103(a) rejection of claim 23, the Examiner respectfully maintains said rejection of claim 23 as cited above.

Art Unit: 2131

Issue 5: With regards to the 35 U.S.C. 101 provisional double patenting rejection of claim 27, said rejection has been withdrawn.

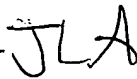
(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Jeremiah Avery – Patent Examiner



Art Unit 2131

(571) 272-8627

Conferees:

Kim Vu – Supervisory Primary Examiner

Art Unit 2135



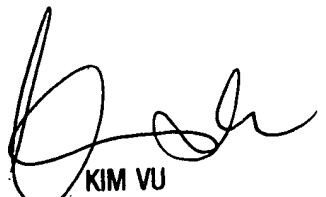
(571) 272-3859

Kambiz Zand – Primary Examiner

Art Unit 2132



(571) 272-3811



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100